INFORMATION REWRITING PROCESS OF SMART CARD

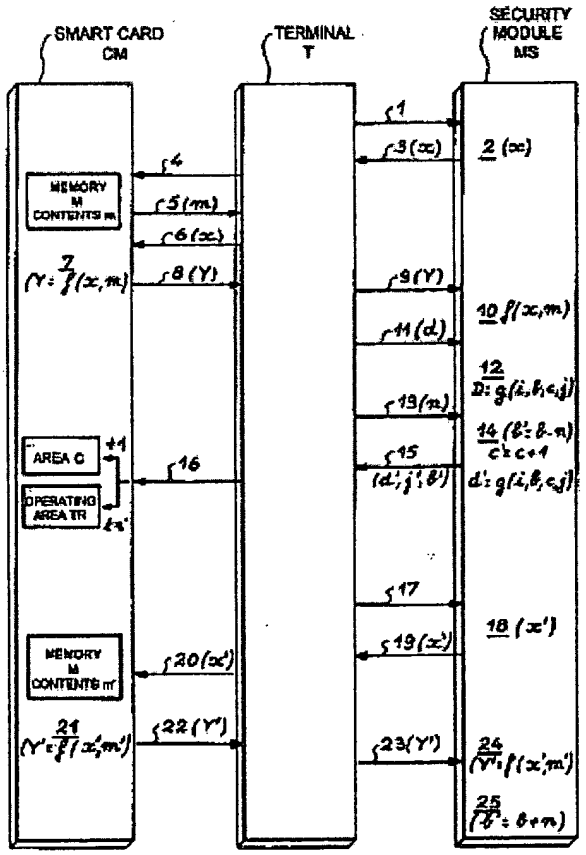
Patent number: JP7110876
Publication date: 1995-04-25
Inventor: JIYANNKUROODO PERE; ERITSUKU DEYUPURE; FUIRITSUPU IOYU
Applicant: CENTRE NAT ETD TELECOMM; POSUTO
Classification:
- international: G07F7/12
- european: G07F7/02C; G07F7/08C; G07F7/08E4; G07F7/10D4E2; G07F7/10D12
Application number: JP19940077562 19940415
Priority number(s): FR19930004515 19930416

Also published as:
EP0621570 (A1)
US5495098 (A1)
FR2704081 (A1)
EP0621570 (B1)

Report a data error here

Abstract of **JP7110876**

PURPOSE: To prevent the illegal use of a card such as transferring money larger than a paid amount from one card, for example.
CONSTITUTION: Concerning this information rewriting process for smart card, an operation for preventing the danger of illegal card usage is added to several operations provided by EP-A-423035. Namely, a memory (M) of the card has a certificate (d), namely, identification (i) of the card, the remainder (b) and prescribed function (g) related to contents (c) of a counter and before updating data, the counter is incremented for '1'. Besides, the certificate (d) is also functioned as a function related to identification (j) of a security module (MS) provided at a terminal.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平7－110876

(43)公開日　平成７年(1995)４月25日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０７Ｆ　7/12				
			Ｇ０７Ｆ　7/ 08	Ｃ

審査請求　未請求　請求項の数４　ＯＬ　（全 5 頁）

(21)出願番号　特願平6－77562

(22)出願日　平成６年(1994)４月15日

(31)優先権主張番号　９３　０４５１５

(32)優先日　1993年４月16日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　592057064
フランス・テレコム・エタブリセマン・オートノム・ドゥ・ドロワ・パブリック
フランス・75015・パリ・プラス・ダレレイ・6

(71)出願人　594024774
ラ・ポスト
フランス・92777・ブローニュ・ビランクール・セデックス・クアイ・ドュ・ブワン・ドュ・ジュール・4

(74)代理人　弁理士　志賀　正武　（外２名）

最終頁に続く

(54)【発明の名称】　スマートカードの情報書き換えプロセス

(57)【要約】

【目的】　本発明によるスマートカードの情報書き換えプロセスは、たとえば１枚のカードから支払われた額以上を引き出させるようなカードの不正使用を防止する。

【構成】　本発明によるスマートカードの情報書き換えプロセスは、ＥＰ－Ａ－４２３　０３５に開示されたいくつかの操作に加えることに、カード不正使用の危険を防止するための操作を追加している。すなわち、カードのメモリー（Ｍ）にカウンタと、認可証（ｄ）すなわちカードの同定（ｉ）、残高（ｂ）、およびカウンタの内容（ｃ）に係る所定の関数（ｇ）とを有しており、データ更新の前にはカウンタが１増分され、また認可証（ｄ）は、端末に備えられたセキュリティモジュール（ＭＳ）の同定（ｊ）に係る関数としても機能する。

にあるように、プリペイドカードにはセキュリティ上の問題がある。この問題は解放型の場合、つまり端末がカード発行機関に対して集金された金額の信頼性を証明する必要がある場合に、特に重要となる。その目的のために、各端末はセキュリティモジュールを備える必要がある。

【０００４】このようなセキュリティ上の問題は、以下のような詐欺の危険を考慮すると、より鮮明となる。

【０００５】危険（ａ）：　交換されたデータの改変：
カードとセキュリティモジュールとの間にデータ処理デバイスを介在させて、たとえば、カードから支払われた以上の額をセキュリティモジュールに登録するように、伝送されたデータを改変することができないようにしておく必要がある。

【０００６】危険（ｂ）：　交換されたデータの再使用：
たとえば、カードからの１回の支払いを基礎にして同一のセキュリティモジュールに対して複数回支払いを行なうように、データ交換を反復させることを防がなくてはならない。

【０００７】危険（ｃ）：　別のセキュリティモジュールの挿入：
第二のセキュリティモジュールを挿入して、１枚のカードからの１回の支払いを基礎に、２つのセキュリティモジュールに支払いを行なわせるようにすることが可能であってはならない。

【０００８】危険（ｄ）：　カードの内容の改変：
カードの購買力を不法に増加すべくカードの内容を改変することが可能であってはならない。

【０００９】これらの問題を解決するには、様々なチェック、データ操作（スクランブリング）、署名確認などを行なうことのできるマイクロプロセッサをカードに導入すればよい。

【００１０】このような解決法は、ある面においては満足のいくものであるが、各カードにマイクロプロセッサを導入しなければならないため、高価であるという不利な点がある。

【００１１】ＥＰ－Ａ－４２３　０３５が開示する電子スマートカードによる支払いまたは情報伝送システムは、マイクロプロセッサの使用を排除している。このシステムは様々な記憶領域をもち、そこには所有者同定情報を持つ領域、認可証を持つ領域、カウンタを持つ領域、残高情報を持つ領域、秘密コードを持つ領域がある。

【００１２】カウンタは、カードによって行なわれる財務操作の回数をカウントする。認可証は、所有者の同定、カウンタの内容、および残高に係る関数である。

【００１３】このシステムは、カードの不正使用を排除することができないという意味で、セキュリティの問題を完全に解決しているわけではない。つまり認可証および残高情報をもつ領域は特に制限なしに消去して書き換えることができる。従って、たとえば１枚のカードから１０点（１０ユニット）分の支払いを行なって、２台の端末に１０点ずつの支払いをさせることによって、１０点分の不当な支払いを作り出すことは防止しようがない。

【００１４】本発明の目的は、この欠点を除去することにある。

【００１５】
【課題を解決するための手段】本発明は上記引用文献によって開示された操作のいくつか（カウンターのカウントアップ、認可証の作成）を採用しているが、その他に、不当な支払いを偽造される危険を防止する操作を追加している。認可証の計算にはセキュリティモジュールの同定が前提となっており、同一のプリペイドカードによる同一の取引操作が２台の異なった端末から行なわれた場合、計算された二つの認可証が必ず異なるようになっている。更に、認可証を消去して書き換えるためには、カウンタの値を一つアップする必要がある。最後に、取引の前後に端末がプリペイドカードとその内容の確認を行なう。

【００１６】より詳しく述べると、本発明はスマートカード（ＣＭ）に含まれたメモリー（Ｍ）の一部分（Ｔｒ）に含まれた情報（ｔｒ）をセキュリティモジュールの備わった端末（Ｔ）によって更新するためのプロセスに関する。メモリー（Ｍ）はカウンタ領域（Ｃ）を有し、更新されるべきメモリー（Ｍ）の部分（Ｔｒ）の内容はその部分（Ｔｒ）の一領域（Ｄ）に認可証（ｄ）を有する。この認可証とは、カードの同定（ｉ）、別の領域（Ｂ）に含まれる残高情報（ｂ）、およびカウンタ領域（Ｃ）の内容（ｃ）に係る関数（ｇ）である。前記プロセスは、カウンタ領域（Ｃ）の内容（ｃ）を１単位分増加してから、メモリー（Ｍ）の部分（Ｔｒ）の更新、部分（Ｔｒ）の旧内容を消去して、その代わりに新しい更新された内容（ｔｒ'）を入力する。また前記プロセスの特徴として、認可証（ｄ）が、最終的更新を行なったセキュリティモジュール（ＭＳ）の同定（ｊ）の関数ともなっており、領域（Ｄ）に含まれる認可証を消去して更新された認可証に書き換えるには、更新の前後にカウンタ領域（Ｃ）がカウントアップされ、端末（Ｔ）がカード（ＣＭ）とその内容（ｍ）を確認する。

【００１７】カードの確認には、データ処理のセキュリティ分野において伝統的手法であるチャレンジ・応答過程が使用できる。端末がカードに、ランダムに選んだ値あるいはすでに使用された値とは異なる値としてチャレンジｘを与えると、カードは次式を計算する。

Ｙ＝ｆ（ｘ，ｍ）

式中、ｍはメモリーの内容を示す。次に端末はＹをチェックするために同じ計算を行なうことによって、カードが本物であること、その内容が正しいことを確認するこ

7

1．TがMSにランダム変数を選択するよう依頼する。
2．MSがランダム変数つまりxを選択して記憶する。
3．MSがxをTへ転送する。
4．TがCMにメモリーMの内容を読むよう依頼する。
5．CMがMを読んでmをTに転送する。
6．TがCMにランダム変数xを使用して自身（CM）を確認するよう依頼する。
7．CMがY＝f（m，x）を計算する。
8．CMがTにYを転送する。
9．TがMSにYおよびmを転送する。
10．MSがf（x，m）を計算して、Yが本当にf（x，m）に等しいことを確認する。
11．TがMSに認可証dをチェックするよう依頼する。
12．MSがD＝g（i，b，c，j）を計算する。
13．TがMSに借り方をnにするよう連絡する。
14．MSが残高の新しい値d'＝d－nを計算し、cをc'＝c＋1にカウントアップして、d'＝g（i，b'，c'，j'）を計算する。
15．MSが更新されたd'，j'，b'をTに転送する。
16．TがCMに依頼して、領域Cに1を書き込み、操作領域Trの内容trを消去し、そこにj'，b'，d'から成る新しい内容を書き込ませる。
17．TがMSに新しいランダム変数を選択するよう依頼する。

8

18．MSがランダム変数x'を選択して記憶する。
19．MSがx'をTにアドレスする。
20．TがCMに、その新しい内容m'によって自身を確認するよう依頼する。
21．CMがY'＝f（x'，m'）を計算する。
22．CMがTにY'の値を転送する。
23．TがMSにY'の正当性をチェックさせる。
24．m'がl'c'，j'，b'，d'に対応すること、およびY'＝f（x'，m'）であることをMSがチェックする。
25．確認結果が正しければ、MSがその残高をn分だけ増加させる。

【0026】先行する複数の操作により、カードの残高が減少し、端末によって集金される額が増加する。この一連の同じ操作が、カードに再度課金して残高を増やして課金する端末の方は同額分減らすことにも使用できることは明らかである。

【0027】上記例において、（m）はカード（M）内のデータの内容を表わす。ただし、認可証（d）のデータおよび残高（b）のデータを（m）に含めないことも可能である。その場合、これらのデータはYが（j）に係る関数である事実によって間接的に確認することができ、実施例の導入を簡素化できる。

フロントページの続き

(72)発明者　ジャンークロード・ベレ
フランス・14610・エプロン・リュ・デ・ルワシール・4

(72)発明者　エリック・デュプレ
フランス・14000・カン・リュ・ガリェイニ・52

(72)発明者　フィリップ・イオユ
フランス・14200・エルーヴィユ・サン・クレール・クアルティエール・グランド・デル・1201